Manager, IT Security (REPOST)
Competition #263-21

Department:	Information Technology	**Salary Range:**	$84,870 - $106,087
Campus:	Barrie	**Classification:**	Administrative
Posting Date:	November 9, 2021	**Status:**	Full-time

Reporting to the Manager, IT Infrastructure, the incumbent is responsible for ensuring appropriate controls are in place for the security of information assets and hardware relied upon by the college's staff. The incumbent ensures procedures and activities comply with all regulatory requirements and internal policies, procedures, guidelines and standards. The incumbent provides leadership to the college community on information security trends and activities. The position also oversees the privacy function for the college ensuring compliance with appropriate legislation. Specific duties include, but are not limited to:

- Acting as the College's subject matter expert on Georgian's response to Information Security trends, vulnerabilities and threats
- Developing, implementing and administering policies, procedures, standards and guidelines
- Evaluating and recommending new information security technologies and counter-measures against threats to information or privacy
- Leading regular security and data privacy reviews, assessments and audits. Identifying, introducing and implementing appropriate procedures including checks and balances, and tests these safeguards on a regular basis
- Providing IT security guidance in the deployment of IT applications and system development projects
- Developing vulnerability assessments and penetration testing for the college's networks and sensitive information systems
- Assessing information security risk through qualitative risk analysis on a regular basis
- Developing data privacy requirements and safeguards to aid various college-wide programs, projects and initiatives
- Developing and executing action plans for completing projects related to the enterprise InfoSec priorities
- Managing numerous complex Cybersecurity projects with various priorities and stakeholders
- Assessing and continuously improving service delivery within cybersecurity program thru effective communications, lessons learned and risk mitigation
- Creating thorough and accurate reports and providing status updates on projects; presenting findings to senior leadership regarding threat identified and recommended security action
- Leading and developing education and awareness programs, and simulated campaigns to ensure workforce are aware of cyber threats, cybersecurity policies, procedures and practices and appropriately informed of their responsibilities
- Overseeing data analysis of incident and threat response; developing and implementing plans to improve procedures
- Creating and implementing Cloud Security Strategy extending governance, control and data leakage prevention, making sure that college's data is protected on SaaS, PaaS and Cloud Application Architecture subprograms
- Developing security architectures for cloud cloud/hybrid systems.
- Leading security scanning/ testing, controls testing, document results, and provide detailed updates to internal stakeholders
- Working closely with the Operation team to provide input and guidance on identity security, zero-day threats, exchange online protection, SharePoint protection, email security, retention policies, device security, MS Teams and other O365 components
- Responsible for Auditing & Reporting, email search, discovery and destroying, and phishing attack simulation
- Providing leadership and supervision to staff by determining work priorities/assignments and approval of staff scheduling
- Human resources management duties include performance review, hiring, team building and conflict resolution
- Conducting first level investigations to resolve disputes involving staff; uses collective agreements, college policies and documents to assist in the dispute resolution process
- Manages staff through review and evaluation of work-in-progress, development of work plans and development of skills and professional currency plans
- Participates in and supervises the preparation and recommendation of detailed budgets with cost estimates. Establishes and maintains budgetary control for the security function including procurement
- Developing and delivering security awareness and training programs

QUALIFICATIONS:

- Successfully completed a four-year degree in computer science, information security or a related discipline
- Completion of a recognized industry certification such as CISSP, CCSP, OSCP, GIAC or other security certifications at a similar level (completed or in progress) is an asset
- A minimum of 7 years progressive IT experience
- Practical experience in the Information Security Architecture field
- Strong understanding of security architecture best practices, standards and frameworks
- Proven experience managing staff and/or leading diverse people through project management
- Possess outstanding communication skills, both oral and written; understand the value of and use persuasive techniques
- Strong experience and detailed technical knowledge in security engineering, system and network security, authentication and security protocols and application security
- Knowledge of network and web related protocols (e.g., TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols)
- Strong understanding of enterprise computing environments including MS Server 2012, 2016 and 2019, Linux, distributed applications, networking, VMWare, Hyper-V, DNS, DHCP, Active Directory
- Strong understanding of nextgen Firewall software, IDS, IPS, virus protection, encryption
- Experience with vulnerability scanning and mitigation utilizing Nessus or similar tool

Georgian College supports diversity, equity and a workplace free from harassment and discrimination. Georgian College is committed to an inclusive, barrier-free recruitment and selection process and workplace. If you are contacted to participate in the recruitment, selection and/or assessment process, please advise the interview coordinator of any accommodations needed with respect to any materials or processes used to ensure you have access to a fair and equitable process.

Alternate formats will be provided upon request throughout the recruitment and selection process.

APPLY NOW:
To be considered for this position, please visit our website at www.GeorgianCollege.ca and apply by navigating to About Us and then to Career Opportunities.

Georgian College has a COVID-19 vaccination procedure in place. As a condition of employment, employees are required to be vaccinated for COVID-19 to work on any campus, or a facility owned, operated or controlled by Georgian College unless they have a valid medical or religious belief/creed reason for not getting vaccinated, which reason will be considered on a case by case basis and which will be subject to the College's accommodation processes.

This position is open until filled. While we thank all applicants, only those contacted for an interview will be acknowledged.